Cisco CyberOps Associate (200-201 CBROPS)

This Cisco Certified CyberOps Associate (200-201 CBROPS) training covers how to act as a member of a Security Operations Center team to prevent and defend cyberattacks on Cisco-enabled networks. This training prepares network engineers to take the 200-201 CBROPS exam, which is the one required exam to earn the Certified CyberOps Associate certification.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Security Concepts — 159 min.

The CIA Triad	7
Comparing Security Deployments Part 1	6
Comparing Security Deployments Part 2	5
Describing Security Terms Part 1	4
Describing Security Terms Part 2	5
Comparing Security Concepts	6
The Principles of Defense In-Depth Strategy	5
Comparing Access Control Models	4
Common Vulnerability Scoring System	6
The 5 Tuple Isolation Approach and Data Visibility	4

Vulnerability and Attack Surfaces

Overview	1
Intro to Vulnerability and Attack Surfaces	1
On-Prem and Cloud-Based Vulnerabilities	10
Zero-day Attacks	5
Weak Configurations	15
Third-Party Risks	2
Lack of Patch Management	11
Vulnerability Management	12
Quiz and Review	7

Data Types for Security Monitoring

Overview	1
Intro to Data Types for Security Monitoring	1
TCPdump Data	17
NetFlow Data	9

	Data from Stateful Firewalls	13

WEEK 2

156 min.

Data from Next-gen Firewalls	10
IPS and IDS Data	8
Data from Security Appliances	6
Quiz and Review	8

Data Obfuscation and Hiding

Overview	1
Intro to Data Obfuscation and Hiding	1
TOR Overview	12
Installing Tails	6
Steganography	8
HTTPS	14
Tunneling	11
NAT-PAT	16
Quiz and Review	6

Network Attacks

Overview	1
Introduction to Network Attacks	1
Wireless Attacks	6
In-line / On-path Attacks	6
Layer 2 attacks	8
Domain name system (DNS)	6
Distributed denial-of-service (DDoS)	4
Malicious code or script execution	2
Remediation Options	5
Review Quiz	8

WEEK 3

Application Attacks

151 min.

Overview	1
Introduction to Application Attacks	1
Injection Attacks	3
Cross Site Scripting	2
Poorly Written Apps	5
Overflow Attack Demo	8
Poorly Written App Attack	4
Impersonation	3
Error Handling Attack	7
Additional Application Attacks	4
Password Recovery Fail	4
Review Quiz	6

Social Engineering Techniques

Overview	1
Introduction to Social Engineering	2
Phishing and Related Attacks	6
Low Tech Attacks	5
Why Social Engineering Works	4
The Top Social Engineering Tool	7
Identifying a Phishing Email	10
Social Engineering Toolkit	8
Review Quiz	5

Cyber Attack Techniques

Overview	1
Introduction to Cyber Attack Techniques	1
Malware	8
Password Attacks	6
Password Attack Example	10
Cyber Physical Components	5
Adversarial AI	4
Supply Chain Security	2
Cryptographic Attacks	4
Review Quiz	8

Certificates and the PKI

Overview	1
Intro to Digital Certificates and the PKI	1

WEEK 4 **156 min.**

Symmetrical vs Asymmetrical Encryption	18
Digital Certificates Overview	7
Digital Signatures	14
Creating an HTTPS Session Key	9
Public Key Infrastructure	11
Quiz and Review	5

Host Based Analysis

Overview	1
Endpoint Security Monitoring Technologies	9
Identifying the Role of Attribution	7
Comparing Disk Images	3
Interpreting Logs	11
Analyzing Sandbox Reports	5

Operating System Fundamentals

Overview	1
Windows Processes and Services	6
Windows Memory and WMI	3
Exploring the Windows Registry	5
Windows Networking	6
Windows File Systems	4
Exploring Linux Processes	4
Linux File Permissions	6
Linux Sudo and Networking	5

Network Intrusion Analysis

Overview	1
Introduction to Network Intrusion Analysis	1
Data Sources	11

WEEK 5 **103 min.**

Event Severity	8
PCAP analysis	14
Extract files from PCAP	9
Regular Expressions	9

Incident Response and Forensic Evidence Collection

Overview	1
Information Security Management Concepts	10

Security Policies and Procedures

Last updated 12.3.2024